STATE MODEL
CLOUD COMPUTING SERVICES SPECIAL PROVISIONS
(Platform as a Service)
IBM's Comments

PaaS Special Provisions Section No.	IBM's Comments
Introduction and general comments	IBM PaaS provides the use of a shared infrastructure across multiple customers with each individual customer's applications located on their virtual hardware resources and operating systems based upon selected usage entitlements. Managed service and the features that are activated depend on the options selected by the customer. Many features described in these terms are activated only if the customer selects the feature. Some are available at an extra cost. These Special Provisions need to reflect the flexibility are contemplated by PaaS. Because of the numerous applications supported and managed under PaaS offerings, IBM cannot commit to all the terms and conditions in this document for all PaaS offered by IBM. For example: Analytics as a Service, Bluemix Development and Test, Cloud Managed Services for Oracle and SAP have numerous options and levels of support for standard, enhanced and premium builds, development and production environments, network connections, DR, and Migration Services. Additionally, similar to the SaaS Special Provision, contractors should have the ability to modify the PaaS Special Provisions in a SOW.
1. Definitions	"Authorized Users" - For PaaS, not all the individuals identified in the definition of "Authorized Users" will have full access to PaaS. Generally, there is a Client Account Administrator/Client Business Point of Contact – responsible for authorized State actions to administer the environment
	"State Data" – IBM uses the term "Content" which is broader than the State's definition of "State Data". IBM suggests that the State consider this broader definitions of "Content" in place of "State Data": all data, software, solutions, products, prototypes technical data and information, including, without limitation, any hypertext markup language files, scripts, programs, recordings, sound, music, graphics,

	images, applets, or servlets that are created, installed, uploaded, or transferred in connection with the Services by the State, users, or solution recipients
	"Security Incident" – Delete "potentially". PaaS is not set up to notify customers of "potential" issues. IBM provides notice when it becomes aware of unauthorized access, not necessarily a potential situation.
	"Service Level Agreement" – Default SLA terms should not apply. SLAs should apply only if part of a Services Description selected. Dispute resolution is not included in the SLA but could be included in a SOW.
3. Data Protection	For PaaS, safeguarding the confidentiality, integrity and availability of State information is subject to the State's control, not the Contractor's control. The State implements the controls that are available to it as features of PaaS selected. a.1 should read "The California Information Practices Act (Civil Code Sections 1798 et seq) applicable to Service Provider as a provider of PaaS" a.2 should read: "Service Provider provides physical security measures for computing environments hosting Cloud Services in accordance with the NIST 800-53 framework." a.3 should read: "Privacy provisions of the Federal Privacy Act of 1974 applicable to Service Provider as a provider of PaaS and only to the extent required by a U.S. governmental agency for this scope of services." 3.c Encryption options available among PaaS vary. The user of PaaS is responsible to determine type(s) of encryption and extent of access control. 3.d Customers will be informed of encryption levels and options, but this generally would not be part of the contract.
4. Data Location	Data centers are located globally. However, if the State wants to use data centers located only in the US, it is the State's responsibility to designate data center locations and the State has control over where data resides or is transferred.
5. Security Incident	Entire Section 5: Flexibility is required. This section should be preceded with "Unless otherwise described in a Service Description or Statement of Work…" 5. a Incident response communication procedures are addressed in selected PaaS offerings, and their security controls and security policy

	management documents. 5.b Most of PaaS offerings are managed services support up to operating system and underlying infrastructure, with various options available for application and database layers managed by the customer, Service Provider, or jointly shared. IBM can agree to provide notification of Security Incidents of which it is aware, but within the control of State's managed portion of the environment, may become aware of a Security Incident before Service Provider is, in which case the State should notify Service Provider. "Immediately" is too stringent. Service Provider needs sufficient time (whether a few hours or several days) to gather facts and determine an incident occurred. Since the State may be aware of an incident first, it is suggest that a more balanced approach be adopted: "In the event either party becomes aware of a Security Incident, such party will promptly (and no more than required under applicable law, to the extent that any such law applies to notifications between a supplier and Box) notify the other party of such Security Incident in writing…" Additionally, notices of Security Incidents go out to all PaaS customers at the same time. We cannot accommodate a different notice schedule for individual customers. 5.c See comments above for 5.b. Not all measures may apply to PaaS. Flexibility is required to adapt these terms to the particular offering.
6. Data Breach Responsibilities	PAAS is managed, so Service Provider does not possess the Content nor control the application or database environment in which it is contained. IBM suggests a more balanced approach for reasons stated above: "In case either party reasonably suspects any loss of, unauthorized access to or unauthorized disclosure of Box Content (each a "**Security Incident**"), such party will promptly (and no more than required under applicable law, to the extent that any such law applies to notifications between a Service Provider and State) notify the other party of such Security Incident in writing (e.g., via email) upon becoming aware thereof and provide sufficient details to enable Service Provider to identify the (suspected) breach and the notified party will provide reasonable assistance to conduct a review of the same. Notice will be made to the mechanisms established for this account. IBM will use standard notification mechanisms as managed by State. State will notify Service Provider through standard mechanisms including but not limited to creating a "Security Issue" Service Ticket or notification to the State assigned Technical Account Manager/IBM Point

	of Contact. The notified party must cooperate fully with the notifying party's reasonable requests for information regarding the Security Incident, and must provide regular updates on each Security Incident and the investigative action and corrective action taken as required.
8. Data Preservation and Retrieval	Generally under the PaaS managed approach the State migrates data in, manages data during steady state and is responsible to migrate out. If State requires assistance from Service Provider, such assistance must be contracted for as additional migration /managed services. Format may vary depending upon offering. IBM may charge for certain transition activities such as delivering content in a specific format. a.b. and c. Flexibility is needed to be modify these sections to adapt them to a particular offering.
9. Background Checks	Replace 9 with: When required under a Statement of Work, and at the State's expense, the Service Provider shall conduct a background investigation in accordance with Service Provider's internal process. These inquiries will include felony/misdemeanor criminal court searched based on all addresses associated with the last seven (7) years of the individual's resident history, including convictions and pending charges. The background report will also include a check of a national criminal database as well as the OFAC Listing. Service Provider's personnel acquired through acquisition may or may not have been screened with recent background checks.
10. Access to Security Logs and Reports	This section is not entirely accurate. PaaS provides State standardized processes and reports as identified in SOW with regard to the IBM controlled and managed environment administering the creation, monitoring and storage of logs under its control. A Cloud Manage Service Delivery model provides limited reference to security logs. Depending upon Service Options chosen may have enhanced capability to create, monitor and store logs. This must be addressed in a SOW.
12. Data Center Audit	Section 12 needs additional details and clarification. IBM recommends the following: Service Provider will arrange for the performance of audits and production of an audit report by an independent third party in accordance with the most recent "Service Organizational Control Type II

	Report" made in accordance with Statements on Standards for Attestation Engagements No. 16 ("SOC2 Report") covering the computing environments used to host Cloud Services. Service Provider will provide a single SOC2 Report covering all computing environment locations hosting Cloud Services. Each SOC2 Report will include an audit of the security, availability and confidentiality of the controls in place for the computing environment and data center physical facilities. An independent third party auditor issues such SOC2 Report at least annually covering operations since the prior SOC2 Report.
13. Change Control and Advance Notice	This depends on the service and must be mutually agreed in a SOW.
14. Security Processes	Delete or further discuss this provision. It is unclear to IBM as to what the State considers as the Service Provider's non-proprietary security processes and technical limitations.
15. Non-Disclosure and Separation of Duties	This provision is unclear. More information regarding the intent is requested.
19. Right to Remove Individuals	Delete as these are individuals that are supporting multiple PaaS accounts and individuals may be critical to support. A better approach would be for the State to raise concerns to Service Provider to address and discuss appropriate measures with the State.``
20. Business Continuity and Disaster Recovery	This section should be deleted or should reference the capabilities that are predefined in the standard products. For PaaS, these services are not customized for individual customers but provide a number of standard options available for specific applications disaster recovery. It is the state's responsibility to determine whether the predefined RTO options available meets their requirements. Alternatively, customized Business Continuity and Disaster Recovery services may provided under a separate SOW.
21. Compliance with Accessibility Standards	Contractors should be required to comply with the Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 only to the extent the law actually applies, i.e, when the service is provided to the Federal government of agency. The General Provisions – IT, Section 7, already require Contractors to comply with applicable statutes, rules, regulations and orders of the United States and the State of California. This Section 21 should not be necessary.
22. Web Services	"The Service Provider shall use Web services exclusively to interface with State Data in near real time when possible." We generally agree that Web services will interface with State Data in near real time when possible. However, there may be situations where we mutually agree to use physical direct tape/hardware to transfer large volumes of data

	to and from web environment instead of over internet would be time prohibitive and impractical. We suggest adding "or as mutually agreed in a SOW."
General Provisions - IT: 16. Inspection, Acceptance and Rejection	Inspection, Acceptance and Rejection does not apply to PaaS. Once the customer purchases PaaS, the service begins and includes a mutually agreed to stabilization period depending upon the complexity of application environment to resolve open issues. There is no ability to reject the service, other than as part of the termination provisions that accompany the service.
General Provisions – IT: 26. Limitation of Liability	Limitation of Liability – Commercially standard limitation is 12 months charges. This should be the limitation on direct damages rather than 1x Purchase Price (which could be for more than one year).
General Provisions – IT: 46. Examination and Audit	The records that will be made available to the State will only be those that document the State's usage of the PaaS. Records relating to multi-tenant usage will not be made available, due to confidentiality concerns.